INTERNATIONAL S[redacted]CH REPORT

Internati[redacted]pplication [redacted]
PCT/IB 03/03120

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
INSPEC, PAJ, WPI Data, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BORST J ET AL: "Cryptography on smart cards" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 36, no. 4, 16 July 2001 (2001-07-16), pages 423-435, XP004304907 ISSN: 1389-1286 page 429, right-hand column -page 430, left-hand column page 431, right-hand column -page 432, left-hand column, line 8	1,2,6,7
Y	--- -/--	3-5

[X] Further documents are listed in the continuation of box C. [ ] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 December 2003	05/01/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat application N
PCT/IB 03/03120

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KARRI R ET AL: "Concurrent Error Detection of Fault-Based Side-channel Cryptanalysis of 128-Bit Symmetric Block Ciphers" PROCEEDINGS OF THE 38TH. ANNUAL DESIGN AUTOMATION CONFERENCE. (DAC). LAS VEGAS, NV, JUNE 18 - 22, 2001, PROCEEDINGS OF THE DESIGN AUTOMATION CONFERENCE, NEW YORK, NY: ACM, US, vol. CONF. 38, 18 June 2001 (2001-06-18), pages 579-584, XP002190412 ISBN: 1-58113-297-2 page 579, right-hand column, paragraph 2 -page 581, left-hand column, paragraph 2 page 581, right-hand column, paragraph 3 -page 583, right-hand column, paragraph 1 ---	1,2,6,7
Y	MENEZES, OORSCHOT, VANSTONE: "Handbook of applied cryptography, PASSAGE" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, CRC PRESS, 1997, pages 334-335, XP002239694 BOCA RATON, FL, USA ISBN: 0-8493-8523-7 page 334, paragraph 9.28 -page 335, paragraph 9.32 -----	3-5